Livestock & Meat Commission
Anti-fraud Policy

1 Introduction

This policy outlines the commitment LMC places on the prevention and detection of fraud and irregularity and provides guidance to staff on these important issues. All public servants are required to act honestly and with integrity, to safeguard resources for which they are responsible. The opportunity to commit fraud is ever-present, and hence must be a concern to all members of staff. It is everyone's responsibility to prevent fraud and follow LMC's procedures where fraud is suspected or detected.

LMC operates a "zero tolerance" policy with regard to fraud. LMC will investigate all instances of actual, attempted and suspected fraud committed by staff, consultants, suppliers and other third parties and will seek to recover funds and assets lost through fraud. Perpetrators will be subject to disciplinary and/or legal action.

1.1 Definition of fraud

The Fraud Act 2006 which became law in Northern Ireland in January 2007 introduced a new general offence of fraud which can be committed in three ways:

- by false representation;
- by failing to disclose information; and
- by abuse of position.

The term "fraud" is commonly used to describe the use of deception with the intention of gaining an advantage, avoiding an obligation or causing a loss to another person or party. Fraud may include such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.

Obviously fraud can be perpetrated by persons outside as well as inside an organisation. The criminal act is the attempt to deceive and attempted fraud is therefore treated as seriously as accomplished fraud.

Fraud can be committed in an infinite number of ways including false representations, altering, concealing or destroying manual or computer records, the misuse of computer facilities or changing computer programmes

Computer fraud is where information technology equipment has been used to manipulate programs or data dishonestly (e.g. by altering, substituting or destroying records, or creating spurious records), or where the use of an IT system was a material factor in the perpetration

of fraud. Theft or fraudulent use of computer time and resources is included in this definition e.g. Internet abuse.

The Fraud Act also established a number of specific offences to assist in the fight against fraud. These include an offence for possessing articles for use in fraud and an offence of making or supplying articles for use in fraud.

2 Responsibilities

2.1 LMC's Responsibilities

The Board's main responsibilities are set out in Managing Public Money Northern Ireland (MPMNI):

- identify, itemise and assess how the organisation might be vulnerable to fraud;
- the development and maintenance of effective controls to prevent and detect fraud;
- to carry out vigorous and prompt investigations if fraud occurs. This will include ensuring that staff who carry out fraud investigations are properly trained;
- to take appropriate legal and/or disciplinary action against perpetrators of fraud;
- to consider disciplinary action where supervisory failures have contributed to the commission of fraud; and
- to establish and maintain systems for recording and subsequently monitoring all discovered cases of fraud.

In the formulation of policy, legislation and related guidance, and in the design of working systems, the Board must ensure that:

- the prevention of loss and fraud is taken into account;
- the risk of fraud and loss are assessed when changes are being considered; and
- weaknesses are identified and rectified when the opportunity arises.

2.2 Accounting Officer Responsibilities

The CEO as Accounting Officer is responsible for establishing and maintaining a sound system of internal control that supports the achievement of LMC's policies, aims and objectives. The system of internal control is designed to identify the principle risks that LMC faces. Managing fraud risk is viewed in the context of managing risk. Although the Accounting Officer bears overall responsibility and is liable to be called to account for specific failures, these responsibilities fall directly on senior and line management and may involve other individual staff.

2.3 Senior Management Responsibilities

Senior Management are responsible for:

- identifying the risks to which systems and procedures are exposed;
- developing and maintaining effective controls to prevent and detect fraud;
- ensuring fraud awareness within the organisation;
- ensuring that controls are being compiled with;

- reporting significant incidents of fraud to the Accounting Officer, reporting to DAERA/DFP and the C&AG in accordance with MPM (NI) Annex 4.7;
- ensuring prompt investigations are carried out if fraud occurs. This will include ensuring that staff who carry out fraud investigations are properly trained;
- taking appropriate legal and/or disciplinary action against perpetrators of fraud, including appropriate action to recover assets;
- taking disciplinary action where supervisory failures have contributed to the commission of fraud;
- establishing and maintaining systems for recording and subsequently monitoring all discovered cases of fraud; and
- providing assurance to the Accounting Officer on their risk and internal control procedures.

2.4 Line Management Responsibilities

Managers are required to:

- identify the risks to which systems and procedures are exposed;
- develop and maintain effective controls to prevent and detect fraud; and
- ensure that controls are being complied with;
- raise fraud awareness amongst staff including knowledge of LMC's anti-fraud policy, and at induction training;
- implement new controls to reduce the risk of similar fraud occurring where fraud has taken place;
- inform Senior Management or the Board when a fraud has occurred or is suspected.

Managers must ensure that opportunities for staff to commit fraud are minimised. In establishing and maintaining effective controls it is desirable that:

- wherever possible there is a separation of duties so that control of a key function does not rest with one individual;
- there is adequate monitoring and checking of outputs;
- backlogs are not allowed to accumulate; and
- staff are adequately trained and have documented procedures available to them.

2.5 Staff Responsibilities

Individual members of staff should:

- act with propriety in the use of official resources and the handling and use of public funds whether they are involved with cash or payments systems, receipts or dealing with suppliers;
- conduct themselves in accordance with the seven principles of public life set out in the first report of the Nolan Committee "Standards in Public Life". They are: selflessness, integrity, objectivity, accountability, openness, honesty and leadership;
- be alert to the possibility that unusual events or transactions could be indicators of fraud;
- alert their line manager where they believe the opportunity for fraud exists because of poor procedures or lack of effective supervision;
- report details immediately through the appropriate channels if they suspect that a fraud has been committed;

- cooperate fully with whoever is conducting internal checks or reviews or fraud investigations;
- assist management in conducting fraud investigations;
- inform management of any outside interest which might impinge on their discharge of duties; and
- inform management of any gifts, hospitality or benefits of any kind offered by a third party as detailed in the Gifts and Hospitality Policy, Bribery Policy and the Staff Code of Conduct where applicable.

2.6 Internal Audit

Internal Audit will evaluate the controls designed to secure assets and data and to prevent and detect fraud, and abuse. The purpose of regular Internal Audit is to ensure that the risk is minimised. Internal Audit is responsible for:

- Delivering an opinion to the Accounting Officer on the adequacy of arrangements for managing the risk of fraud and ensuring that the organisation promotes an anti-fraud culture;
- Assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk in LMC's operations; and
- Ensuring that management has reviewed its risk exposures and identified the possibility of fraud as a business risk.

2.7 Audit and Risk Assurance Committee

The Audit and Risk Assurance Committee is responsible for advising the Accounting Officer and Board on:

- Management's assessment of the organisation's risk from fraud and the appropriateness of their response to it; and
- The organisation's anti-fraud policies and arrangements, whistleblowing procedures and arrangements for investigations.

3 Reporting suspicions

There are various signs and indicators that are clues that fraud may be taking place. Some indicators relate to staff themselves and others to actual work performance and working procedures.

Examples of indicators include:

- Unusual employee behaviour.
- Unrecorded transactions or missing records (e.g. invoices, contracts).
- Absence of controls and audit trails (e.g. inadequate or no segregation of duties, lack of rotation of duties).
- Inadequate monitoring to ensure that controls work as intended (periodic testing and evaluation).
- Documentation that is photocopied or lacking essential information.
- Alterations to documents.

- Unsatisfactory explanations of actions taken.
- Expected expenditure exceeded.
- Falsification of management information documents.
- Suppliers / contractors who insist on dealing with one particular member of staff.

A full list of indicators can be located in Appendix 1.

The Public Interest Disclosure Act 1998 protects employees who raise concerns about certain matters of public interest in good faith. LMC has established procedures to encourage staff to report actual, attempted or suspected fraud and/or other forms of illegal activity without fear of reprisal.

Staff should not attempt to investigate any fraud themselves.

4 Fraud Response Plan

LMC has in place a Fraud Response Plan which can act as a checklist of actions and a guide to follow in the event of either internal or external fraud being suspected.

4.1 Plan

4.1.1 Staff must report details immediately to their line manager or next most senior person if they suspect that a fraud has been committed or see any suspicious acts or events. Staff should also assist in any investigations by making available all relevant information and by co-operating in interviews. Staff may also refer to LMC's Whistleblowing Policy for further guidance.

4.1.2 Irrespective of the source of suspicion, managers must undertake an initial investigation to determine the facts. This investigation should be carried out as speedily as possible and certainly within 24 hours. The purpose of the initial investigation is to confirm or repudiate the suspicions that have arisen so that, if necessary, further investigation may be instigated. The Chief Executive should be advised of the position in advance of the preliminary investigation.

4.1.3 Preliminary investigation may involve discreet enquiries with staff or the examination of documents. It is important for staff to be clear that any irregularity of this type, however apparently innocent, will be investigated.

4.1.4 If initial investigation confirms the suspicion that a fraud has been perpetrated, then, to prevent the destruction of evidence that may provide essential support for subsequent disciplinary action or prosecution, management should take steps to ensure that all original documentation is preserved in a safe place for further investigation. If the removal of documents would impair the efficient operation of work, management should arrange for copies to be made for continued use while retaining the originals.

4.1.5 In addition, any member of staff involved in suspected fraud may be suspended pending the outcome of the investigation. Suspension itself does not imply guilt; it is another safeguard to prevent the removal or destruction of evidence and to avoid repetition of the offence.

4.1.6 If, after investigation, management is satisfied that a prima facie case of fraud has occurred, LMC will consider the appropriate course of action. In addition the Chief Executive will report the matter to the Central Investigation Service (CIS) within the Department of Agriculture and Rural Development. The CIS may refer the matter to the NIAO, PSNI and DFP.

4.1.7 LMC will take all necessary steps to recover assets and this may include the freezing of assets, obtaining search orders and the prevention in releasing assets.

A Memorandum of Understanding (MOU) has been developed between the Northern Ireland Public Sector and the Police Service of Northern Ireland (PSNI). The MOU sets out the framework for the working relationship between LMC and the PSNI in respect of the investigation and prosecution of suspected fraud cases. The MOU is available at http://www.dfpni.gov.uk/index/finance/afmd/afmd-corporate-governance/afmd-fraud/mou_-_public_sector_and_psni.pdf

The acceptance criteria and agreed format of evidence pack provides guidance on the procedures to follow when formally referring a suspected fraud case to the PSNI and can be obtained directly from the PSNI.

For additional guidance the Head of Counter Fraud activities (Jim Armstrong) can also be contacted on 028905 25008 Jim Armstrong@daera-ni.gov.uk.

5 Conclusion

While the circumstances of individual frauds will vary, it is important that all are vigorously and promptly investigated and that appropriate action is taken. LMC views fraud very seriously.

This policy is endorsed by the Commission and is reviewed regularly. You are encouraged to raise concerns at an early stage wherever possible.

Appendix 1 – List of Fraud Indicators

- Unusual employee behaviour (e.g. a supervisor who opens all incoming mail, refusal to comply with normal rules and practices, fails to take leave, managers by-passing subordinates, subordinates by-passing managers, living beyond means, regular working of long hours, job dissatisfaction/unhappy employee, secretiveness or defensiveness).
- Unrecorded transactions or missing records (e.g. invoices, contracts).
- Disorganised operations in such areas as accounting, purchasing or payroll.
- Crisis management coupled with a pressured business environment.
- Absence of controls and audit trails (e.g. inadequate or no segregation of duties, lack of rotation of duties).
- Low levels of review or approval.
- Policies not being followed.
- Inadequate monitoring to ensure that controls work as intended (periodic testing and evaluation).
- Lack of interest in, or compliance with, internal controls.
- Documentation that is photocopied or lacking essential information.
- Alterations to documents.
- Missing documents such as expenditure vouchers and official records.
- Excessive variations to budgets or contracts.
- Bank and ledger reconciliations are not maintained or cannot be balanced.
- Excessive movements of cash or transactions between accounts.
- Numerous adjustments or exceptions.
- Duplicate payments.
- Large payments to individuals.
- Unexplained differences between inventory checks and asset or stock records.
- Transactions not consistent with the entity's business.
- Deficient screening for new employees including casual staff, contractors and consultants.
- Employees in close relationships in areas where segregation of duties is a key control.
- Unauthorised changes to systems or work practices.
- Lowest tenders or quotes passed over with minimal explanation recorded.
- Single vendors.
- Unclosed but obsolete contracts.
- Defining needs in ways that can be met only by specifi c contractors.
- Splitting up requirements to get under small purchase requirements or to avoid prescribed controls.
- Suppliers/contractors who insist on dealing with one particular member of staff.
- Vague specifications.
- Disqualification of any qualified bidder.
- Chronic understaffing in key control areas.
- Excessive hours worked by key staff.
- Consistent failures to correct major weaknesses in internal control.
- Management frequently override internal control.
- Lack of common sense controls such as changing passwords frequently, requiring two signatures on cheques or restricting access to sensitive areas.